

**Testimony of Robert Holleyman
President and CEO
Business Software Alliance**

Before the House Committee on Foreign Affairs

**Hearing on
The Google Predicament: Transforming U.S. Cyberspace Policy to
Advance Democracy, Security, and Trade**

March 10, 2010

Good morning. My name is Robert Holleyman. I am the President and CEO of the Business Software Alliance.¹ BSA is an association of the world's leading software and hardware companies. BSA members create approximately 90% of the office productivity software in use in the U.S. and around the world. We appreciate the opportunity to testify today on issues that are important to our member companies.

BSA member companies are committed to fully harnessing the power of the Internet and cyberspace. This is a unique time. Computers and software have transformed our lives at home and abroad. They empower individuals, business and nation states in ways that are now taking shape but are not yet fully shaped. The challenge confronting each of us, and especially this Committee, is ensuring that cyberspace contributes its full measure to the common welfare of all people.

BSA member companies confront three challenges in pursuing this goal. First, intellectual property (IP) theft is a huge and growing problem that harms our entire economy. Promoting and protecting innovation is vital to the software and IT

¹ The Business Software Alliance (www.bsa.org) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Altium, Apple, Autodesk, AVG, Bentley Systems, CA, Cadence, Cisco Systems, CNC/Mastercam, Corel, Dassault Systèmes SolidWorks Corporation, Dell, Embarcadero, HP, IBM, Intel, Intuit, Kaspersky Lab, McAfee, Microsoft, Minitab, Parametric Technology Corporation, Quark, Quest Software, Rosetta Stone, SAP, Siemens, Sybase, Symantec, Synopsys, and The MathWorks.

industries. IP laws by purpose and design provide incentives to create and innovate. Countries that tolerate the theft of intellectual property are killing innovation. They are also engaging in unfair trade practices that harm our country by robbing us of much-needed jobs. While the US has taken a leadership role in combating theft of intellectual property, the problem for software remains acute and persistent. We should take a hard look at both international and domestic laws to determine what can be done.

Second, full utilization of the Internet requires that its shape and contours be determined by ingenuity and the drive to use and share information. Policies that seek to bend these developments to the contours of a specific country's industrial development goals are far more likely to cause impediments. Policies requiring innovation to be done within a country's territory to fully enjoy market access, pose a particular threat of Balkanizing global innovation.

Finally, cyber crime is preventing the Internet from reaching its full and considerable potential. The Internet is at its most basic level about relationships between information providers and users of the information. This relationship is built on mutual trust. And that trust is nourished when there is a sense that the information shared and exchanged is secure from misuse and tampering. Thus, ways to increase trust and security is an indispensable component of sound cyberspace and Internet policy. I urge this Committee and the Congress to take a fresh look at all three challenges.

In my testimony, I will give a brief overview of the business software industry and its role in our economy and society. I will describe how the inaction of national governments in the face of massive theft of intellectual property creates real, immediate threats to American jobs and our economy, and propose measures that can be taken to reduce IP theft. I will then describe the increasing trend towards restricting market access and trade challenges that the software industry faces around the world. These challenges include policies that seek to exclude US and other foreign companies from large segments of the market and compel transfers of research and development and IP. Finally, I will discuss the software industry's commitment to security in cyberspace, the security threats we now confront on the Internet and the specific steps that we recommend the United States and all other countries take to address the problem.

Overview of the Software Industry

Software and computers have changed the world in which we live. It has made us more efficient, more productive and more creative. Software and computers deliver better results in dealing with national priorities such as health care, energy, infrastructure, education, and e-government. Software has been at the heart of this technology revolution. Software drives productivity and innovation in almost every economic sector, helping businesses of all sizes perform better in good times and bad. It makes our lives easier, more connected, and more fun at home.

The software industry has also proven to be a remarkable engine for jobs and economic growth. The software and related services sector employed almost 2 million people in the US in 2007 in jobs that, on average, paid 195% of the national average. This sector contributed more than \$261 billion to US GDP in 2007, making it the largest of the US copyright industries.

Without question, the software industry's direct contribution to our nation's economic health is significant. That's not the whole story, though. Remember that much of the prosperity that the US enjoyed, beginning in the second half of the '90s, was built on increased productivity. Information technology, including software, has been the essential driver of these productivity gains.

Software also lies at the heart of the solutions to a whole host of other challenges we face. Green building design, smart electrical grids and electronic health records are a few of the solutions that depend on software. Today – right now – software is helping to teach essential skills to students, to find the most energy-efficient way to get goods to where they're needed and, quite literally, to heal the sick and injured.

Intellectual Property Theft

All of these benefits from a healthy, innovative software industry are imperiled by the simple decision to use software without paying for it. This decision, when repeated by consumers and businesses millions of times throughout the world, has a staggering cumulative effect. One in five copies of PC software in use in this country in 2008, valued at more than \$9.1 billion, was stolen. And we have the lowest rate of PC software piracy in the world. Globally, the rate is forty-one percent. That translates into the theft of software worth nearly \$53 billion in a single year.

Those who steal software are stealing jobs and tax revenues. A study conducted for BSA by IDC last year found that lowering software piracy rates stimulates the entire IT sector, creating jobs and increasing economic growth and tax revenues. The study concluded that a global 10-point reduction in PC software piracy over four years would deliver an additional 600,000 new jobs, \$24 billion in tax revenues, and \$141 billion in economic growth.

Reducing piracy delivers indirect benefits as well. Society benefits from new technological innovations. Consumers benefit from more choices and greater competition. Internet users benefit from new ways of communication and expanded creative content made available online. And national economies benefit from enhanced productivity leading to higher standards of living.

The business software industry's most harmful piracy problem traditionally has involved its primary users – large and small corporate, government and other enterprises – that pirate our members' products by making additional copies of software for their own internal usage without authorization. We commonly refer to this activity as "organizational end-user piracy." While we face other forms of piracy, such as pirate CDs and illegal downloads, organizational end-user piracy causes by far the greatest economic harm to our industry.

Organizational end-user piracy occurs in many different ways. In what is perhaps the most typical example, a corporate entity will purchase one licensed copy of software, but will install the program on multiple computers. Other forms of end-user piracy include copying disks for installation and distribution, in violation of license terms; taking advantage of upgrade offers without having a legal copy of the version to be upgraded; acquiring academic or other restricted or non-retail software without a license for commercial use; and swapping disks in or outside the workplace. Client-server overuse – when too many employees on a network have access to or are using a central copy of a program at the same time, whether over a local area network (LAN) or via the Internet – is another common form of end-user piracy.

Organizational end-user piracy goes on in enterprises large and small, public and private. These enterprises receive the productivity benefits that the software provides, while foregoing the expense of licensed copies of the software. Not only do they steal from software producers, in effect these enterprises enjoy an unfair commercial advantage over their law-abiding competitors who must make a choice between paying for software or doing without.

This unfair commercial advantage operates at an international level as well: On average, enterprises in countries with high rates of software piracy are competing unfairly with enterprises from countries with low rates of software piracy. To give a particularly stark example, China's 80 percent software piracy rate means that 4 out of 5 enterprises in China can compete unfairly with enterprises in the US that are paying for the software they use to run their businesses and improve productivity.

I want to urge us all to begin thinking of the problem of intellectual property theft in a different way. The problem is more pervasive, more complex, and more pernicious than it was just a few years ago. Quite frankly, the term "piracy" is outdated. It does not even begin to capture the breadth of the problem. This problem has dire implications for America's future well-being.

There are a number of steps that BSA recommended to Vice President Biden in connection with his December 2009 roundtable discussion on piracy and counterfeiting that the federal government could take to address the problem of IP theft:

Executive Order

The federal government can have a profound effect on software theft through its role as a procurer of goods and services. Under Executive Order 13103 of September 30, 1998, federal agencies must take steps to ensure that they use only legal copies of software. That principle could be extended by executive order to require that federal contractors also use only legal copies of software. Firms that seek to sell goods and services to the US government should certify that their use of software is in compliance with the Copyright Act and relevant license agreements, and that they have controls in place to ensure that this is so. This action by the Administration would establish a standard for other governments to follow.

Legislative Action

The enactment of the PRO-IP Act in 2008 provided the federal government with a range of new tools and resources to coordinate and enhance intellectual property enforcement efforts. BSA supported this important legislation and looks forward to working with you and other officials in its implementations. At this time, we are reviewing with our members potential options for legislative reform beyond those

contained in the PRO-IP Act, and will be back in touch with the Committee with any additional recommendations.

We note that there has been a great deal of discussion about the asserted need for a “graduated response” or “three strikes” legislation to address some forms of Internet piracy. This is legislation that would require ISPs to take a series of steps in response to allegations of copyright infringement by their subscribers, ultimately leading to sanctions against subscribers who are deemed repeat infringers.

While we support taking action against repeat offenders, as we have learned from similar efforts in France and elsewhere, it has proved very challenging to find a legislative approach that effectively deters online piracy while respecting users’ rights and interests, and safeguarding the myriad legal activities that require access to the Internet. These include such increasingly indispensable activities as online banking, monitoring a child’s progress in school, managing one’s health care and receiving instantaneous alerts concerning natural disasters and other threats.

Whether in the US or abroad, BSA supports action by ISPs against repeat infringers. We believe that this is responsible action that should be taken on a voluntary basis, and is wholly consistent with existing obligations under law in many jurisdictions. When it comes to government policies that require ISPs to impose sanctions, including potentially the suspension or termination of Internet access, it is important that appropriate safeguards – particularly due process protections – are put into place to protect subscribers. BSA members have articulated a set of key principles on graduated response that we attach for the record.

Cooperation with Trading Partners

Cooperation with our trading partners is essential. As we have noted, software theft is by far the largest form of piracy in dollar terms and by many accounts constitutes 75 percent of worldwide piracy of US copyrighted works. Moreover, because software is integral to economic and business activity, its impact is far greater than the direct losses through theft would suggest.

With these facts in mind, we have four initial recommendations on international initiatives.

First, establishing requirements for the use of legal software by all governments and their contractors would have an immediate positive impact. In virtually every country, the government is the single largest customer of software. Government policies have a substantial effect in shaping local markets, and establishing requirements for legal use by contractors and governments would have a profound positive effect on deterring corporate and institutional end user piracy.

Second, we urge establishing international regimes to address the unfair trade practices that result from governments' tolerance of software theft, which provides unfair competitive advantages to those companies who operate with stolen software. It is our sense that the trade distortions and job losses that arise from software theft should be subject to specific rules under international trade laws. Thus, we would urge you to examine ways to make such practices subject to WTO disciplines as well as disciplines under bilateral trade agreements and relevant national laws.

Third, move ahead as expeditiously as possible to conclude a meaningful Anti-Counterfeiting Trade Agreement (ACTA). Gaining the commitment of key trading partners to obligations consistent with the strong substantive and enforcement provisions reflected in U.S. law and practice is itself valuable. Moreover, the potential for ACTA to provide a mechanism for further cooperation among governments in enforcement efforts and the development of best practices offers important opportunities.

Finally, with respect to organized criminal counterfeiting of business software we urge government investment in criminal and Internet enforcement resources to intercept and shut down the illicit counterfeit software trade both domestically and overseas. This should include focus on re-importation of counterfeit software for resale on domestic internet sites.

Challenges in the China Market: IP Theft and Technology Nationalism

Although the challenges I have just described are present in many countries around the world, I would like to say a few words about the challenges BSA members confront in China, to illustrate the point.

China is a critically important market for BSA companies. It is already the second largest market in the world for personal computers, and it is growing much faster than

developed markets like the US, Europe and Japan. BSA companies are fully committed to the China market and seek to work cooperatively with the Chinese authorities. Most of our members have a presence in China, and many have made substantial investments there.

But China is a market with real challenges – challenges that act as significant barriers to trade. Pervasive, intractable IP theft (estimated at 80% for the PC software sector) deprives US software companies of literally billions of dollars each year, and allows Chinese enterprises to compete unfairly with businesses here in the US. Government policies on technology and procurement act as a further brake on our companies' ability to do business in China. These are issues that require direct engagement to protect US interests and ensure that China lives up to its responsibilities as an economic power and a member of the global trading community.

In addition to its excessively high level of software piracy, China has pursued several policies over the past year that have an adverse impact on the ability of US and other technology firms to do business there.

China's effort last year to mandate use of specific software to filter Internet content – the so-called "Green Dam" controversy – threatened to play havoc with the increasingly interdependent hardware and software systems that comprise the Internet in China. Fortunately, the government of China reconsidered that policy after intervention by businesses and governments on both sides of the Atlantic and the Pacific.

However, a broader challenge faces our industry from China's increasing efforts to implement policies to promote "indigenous innovation" that discriminate against foreign firms and seek to compel them to transfer IP rights to Chinese ownership.

For example, this past November the Chinese government took steps that will essentially close the government market to US and other non-Chinese providers of software and other innovative technologies. Companies in six critical sectors, including software, telecommunications, and energy-efficient products were given a December 10, 2009 deadline to apply to get on a list of preferred products the Chinese government will buy. The criteria for a product to be listed includes requirements that the product contain IP that was developed and owned in China and that its original trademark be registered in China. We believe that few, if any, US companies will qualify unless they turn over their IP to a Chinese entity. This could amount to a

potentially massive transfer of IP, jobs and economic power. Mr. Chairman, that is a step that is not in our national interest or in the interest of US companies.

In December, the Chinese government issued another directive that extends government procurement and other preferences for indigenous products to 18 other industry sectors, including heavy machinery. The scope of these efforts affects US companies across many critical sectors that are vital to US economic growth and job creation. These efforts run counter to Chinese commitments to open trade and investment – commitments they have made in various bilateral fora including last year's summit between President Hu and President Obama. We appreciate the strong letter you sent to the Chinese Ambassador raising concerns about these policies.

While I have highlighted policies related to government procurement, I would note that China's efforts to discriminate against foreign companies and compel IP transfers extends to policies related to patents, standards, information security products and other areas.

We believe these discriminatory policies by the Chinese government require an intensified and coordinated response from the Administration. A few weeks ago, BSA joined with 18 other industry associations from the technology and broader business sectors on a letter to Secretaries Clinton, Geithner and Locke, Attorney General Holder and US Trade Representative Kirk urging the Administration to elevate these issues to a strategic priority in our bilateral economic agenda with China.

Security in Cyberspace

BSA member companies are leaders in promoting cyber security. They recognize that electronic commerce, which is so vital to our industry and to the economy as a whole, cannot reach its full potential without the trust of consumers and businesses.

I believe that we can draw several important lessons from the cyber intrusions and attacks experienced by Google. First, this was not a unique event. A broad range of companies, including BSA members, has been and will continue to be targeted for cyber intrusions and attacks. In the realm of cyber crime, cyber industrial espionage and other intrusions and attacks, BSA member companies are on the front lines. This highlights the critical importance of having sound commercial security practices in place. It is not merely a business imperative – it is vital to our nation's economic security.

Second, security in cyberspace is a matter of concern for any country that uses innovative technologies. Security readiness is both a matter of national and economic security. But it is also a matter of good global citizenship in an era of increasing interconnectedness. Governments need to establish both good policies and good practices. There are several steps that BSA recommends.

First, governments should enable individuals and companies to deploy the security measures necessary to protect their electronic information and systems. In this fast-paced game of cat and mouse, we must not pin computer users down behind static and rapidly outdated Maginot lines. This means governments should not require the acquisition or deployment of specific products or technologies including specific hardware or software and instead should permit the acquisition and use of internationally-accepted cyber security tools, solutions and approaches. It also means that governments should permit the use and deployment of security measures based on internationally accepted standards. Mandates of specific types of technologies, or domestic standards that diverge from international standards, only serve to weaken protection and diminish trust.

Second, governments should institute a legislative or regulatory framework that will provide overall guidance for businesses and consumers with respect to privacy. This can be either a comprehensive data protection framework or sector-specific legislation. Such governmental action will complement other mechanisms such as technological solutions, industry best practices, and consumer education to bring about a safer online environment. Any such framework should be consistent with OECD privacy principles and the APEC privacy framework. It should also require covered entities to develop, implement, maintain and enforce reasonable administrative, technical and physical safeguards, appropriate to the size and complexity of the entity, the nature and scope of its activities, and proportional to the likelihood and severity of the potential harm.

Third, governments should require that organizations notify individuals when the security of their personal data has been breached. However, not all breaches should be notified, to avoid creating undue alarm. When a breach of security has created a significant risk that the data will be misused, the affected consumers should be notified, so that they can take mitigation measures. Additionally, such notification requirements should exempt breaches where the affected data had been rendered unusable, unreadable or indecipherable to an unauthorized third party through the use

of practices or methods such as encryption, redaction, access controls and other such mechanisms that are widely accepted as effective industry practices or industry standards. To do this in the US, BSA supports H.R. 2221 as passed by the House, and S. 1490 as passed by the Senate Judiciary Committee, both of which adhere to these principles.

Fourth, governments are under regular and persistent cyber attack from criminals and hostile nations. Therefore, they should implement best in class security to protect their own computers, networks and systems. For U.S. federal agencies, this means urgently reforming the Federal Information Security Management Act (FISMA). This 2002 law was an important milestone in the effort to elevate information security among the management priorities of federal agencies. However, FISMA has not improved information security as much as it was hoped. Agencies can comply with FISMA and yet still have significant gaps in their actual security, because FISMA only requires that they show they have security processes in place, without ensuring that these measures effectively lead to mitigating the cyber risks that the agency actually faces. Congress needs to reform FISMA, to ensure that agencies have the authority and resources to identify and mitigate the cyber risks they actually face. Senator Carper is putting the finishing touches to his bill – S. 921, the United States Information and Communications Enhancement Act. We believe S. 921 will focus more narrowly on consensual FISMA reform provisions when it moves in the Senate Homeland Security and Governmental Affairs Committee, and if it does we will support it in that form. We understand that the House Oversight and Government Reform Committee is also working on reforming FISMA. There is broad consensus among stakeholders about how best to reform FISMA, and we are optimistic that the Oversight and Government Reform Committee will act on it.

Fifth, governments should crack down on cyber crime. BSA urges all governments to consider ratifying the Council of Europe Cyber Crime Convention. This treaty, which the United States ratified in 2006, is the only international instrument that prohibits cyber crime and provides for international law enforcement cooperation against it. It is a foundational component of international cyber security. To assist countries that may not be ready to ratify the Council of Europe Convention, BSA has drafted a model law that can be used to bring their domestic criminal laws up to international standards. It is important to recognize, however, that laws are insufficient without appropriate enforcement. Governments need to effectively enforce their cyber crime laws and their law enforcement agencies must cooperate with their foreign counterparts, to ensure their territories do not become safe havens for cyber criminals. To do this, countries

need dedicated and knowledgeable investigators, prosecutors and judges, with adequate resources, and the ability to hand out deterrent penalties.

Sixth, countries should enact legislation or adopt regulatory measures to facilitate the voluntary sharing of cyber security information between the government and private sector (e.g. actionable threat and vulnerability information, or incident response plans). Such voluntary information sharing promotes the protection of critical information infrastructure, most of which is owned and run by the private sector.

And **seventh**, governments need to educate the public – home users, children and small businesses in particular – about “cyber hygiene”, “safe” and “ethical” computing. This includes education about software piracy, because a lot of risks to the public come from the use of pirated software. Governments should tap industry resources for such efforts because industry, and the information technology industry in particular, have invested a lot into cyber security education.

These seven recommendations form the core of what we recommend the United States government pursue as its international cyber security strategy.² We believe such a strategy should address the full range of cyber security issues. Most importantly, its year-round implementation by the various relevant federal agencies should be led by the White House Cybersecurity Coordinator and be well-resourced.

Conclusion

Software contributes profoundly to the world in which we live. It allows us to share, to create and to innovate in ways previously unimaginable. Software-driven productivity strengthens national economies, including our own, and makes them more competitive and more prosperous. Unfortunately, software theft, technology nationalism and cyber crime prevent the software industry from realizing its full potential.

Thank you again for the opportunity to testify here today. I look forward to your questions and to continued dialogue on this important topic in the future.

² The Cyberspace Policy Review, released by the White House on May 29, 2009, recommended the development of “*U.S. Government positions for an international cybersecurity policy framework*” and strengthening “*our international partnerships to create initiatives that address the full range of activities, policies and opportunities associated with cybersecurity.*” (Cyberspace Policy Review, p. vi, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)

BSA Position on
Appropriate Measures to
Deter On-Line Piracy of Content

On-line piracy presents a serious and immediate threat to software developers as well as other copyright based industries. Too many persons now treat illicit acquisition of copyrighted works on-line as a routine matter, ignoring the fact that they are engaging in illegal acts. But it is important not to lose track of the fact that the vast majority of individuals and businesses use software, computers and the Internet for a myriad of legal and legitimate personal and business reasons.

The current voluntary industry-led approach to developing technologies to address on-line content piracy continues to be effective and mandated use of any such technologies is not justified. Measures taken should be tailored to the content piracy issue identified and Government's role should be to ensure that legal offerings for digital content services are facilitated.

BSA members approach proposed solutions to address on-line content piracy with two objectives:

1. To effectively deter illicit downloading, uploading, making available and use of content; and,
2. To ensure existing technologies function as designed, that innovation and the development of new technologies and services are not obstructed, and that users' enjoyment of software, computers and the Internet is not diminished.

BSA members believe due care must be taken to ensure policies meet both considerations. We believe the following principles provide the basis for achieving this balance.

1. Some anti-piracy content identification and filtering technologies may play a useful role in deterring piracy in some limited cases, but they are not a "silver bullet" solution to piracy. Rather, addressing piracy effectively requires ongoing voluntary inter-industry efforts.
2. In appropriate circumstances, BSA supports:
 - a. Automated educational notification mechanisms for alleged online infringers and a requirement for ISPs to preserve evidence of repeated infringements such as a users' IP address to enable anti-piracy court proceedings and administrative anti-piracy procedures or appropriate enforcement actions, subject to appropriate safeguards, including those governing privacy;
 - b. The imposition of appropriate sanctions, including blocking a user, blocking a site, and the suspension or termination of Internet service for individual repeat offenders, provided:
 - i. Such sanctions against individual repeat offenders shall be based on either:
 1. Breach of contract, i.e., the terms of subscriber's contract with the service provider. (Contractual mechanisms are a helpful and efficient way of dealing with on-line piracy and should be encouraged and widely implemented.)
 - or
 2. Through a decision by an administrative or judicial entity, provided such entity gives all parties an opportunity to be heard and present evidence, and that the decision can be appealed before an impartial court. Before an order becomes final, parties shall have the opportunity to have the order stayed pending appeal to courts.

3. When developing steps to address on-line content piracy the following shall also be given due consideration:
 - a. The voluntary development and use of anti-piracy content identification and filtering technologies should continue unimpeded: this self-regulatory approach is the effective way to address piracy. The specific technologies themselves should be developed through voluntary processes open to all affected stakeholders, and the results should be based on consensus of the participants.
 - b. In specific cases where anti-piracy content identification and filtering technology is used, it should be demonstrated to be robust, renewable, interoperable, free of unintended consequences for existing systems and any other relevant criteria necessary to ensure users experience will not be degraded and the development and deployment of new technologies will not be impeded.
 - c. Where it is determined that it is necessary to empower national judicial or administrative entities to require the use of anti-piracy content identification and filtering technologies, such entities shall impose the requirement as a remedy on a case by case basis, in view of the specific facts presented, and after all affected stakeholders have had an opportunity to assess the impact of the specific anti-piracy content identification or filter's use on their technologies, and identified issues have been comprehensively addressed.
4. BSA opposes:
 - a. The termination of ISP services or any other sanctions or penalties imposed on alleged infringers without due process and, at a minimum, a right of appeal to a judicial authority, except when such penalties are imposed as a result of a breach of contract with the service provider.
 - b. Imposition of broad anti-piracy content identification and filtering technological requirements applicable to all Internet users, or all computers and software used to access the Internet, by legislation, administrative fiat or adjudication.